

December 9, 2010 NIST Smart Grid Privacy Subgroup Meeting Notes

Minutes by Rebecca Herold

Please send this distribution list any necessary corrections or additions.

Next full group teleconference meeting:

Thursday December 16, 2010 at 11:00am est

Here are my summary notes from the meeting:

1. Info on NAESB (North American Energy Standards Board) – Tanya

- At Grid Interop. A push for model language on a number of topics that could be useful for regulators to use. One of best places to start is privacy.
- NAESB has had a lot of push internally to do a business practices document (voluntary) addressing with privacy issues.
- They are looking at our Vol 2 (within NISTIR 7628) as a starting point to use when creating the business practice document. A few weeks away.
- What is likely is an effort for our group to assist the NAESB group in creating the business practices group. May turn into a full-fledged PAP.
- If that happens then we'll have a very wide audience for the work. There will be other groups involved at
- Chris K: As a NAESB member (and former state regulator), one big advantage of having NAESB publish a business standard is that many/most state commissions will use it as a basis for rulemaking or simply refer to it. It is voluntary effort until after the state commissions say you must do.

2. Team reports

- Privacy Use Cases Team: Christine Hertzog (team lead):
 - Did not make the call this morning.
- Third Party Team: Brent Struthers, Neustar (team lead)
 - Tanya has provided the first working document that takes the first principle (accountability) and looks at the security requirements that are applicable and documents if it needs adjustment.
 - The list for the first one has been made.
 - Will meet Monday next week and will work through the language that will be the additional privacy considerations for each of the requirements.
 - Will then note any gaps.
 - With the first one basic wording changes will be made.
- PEV Team: Mike Coop, Hey Coop! (team lead)
 - Came out of Grid Interop. PAP 11 has been shut down. The outstanding issues will likely be pushed to PAP19.
 - Excited about the security piece and is looking for a co-lead for that.
 - Will likely have a call next Wednesday.
 - Looking at the roaming issues. What is roaming? E.g., if you leave PG&E land and enter another land (Santa Clara), from a billing standpoint, if you plug into a friend's house, will you get back to your home account, or will your friend get charged?
 - Not much has been done with the roaming concerns. Very few people have thought about it. No one knows if it will be an issue or not. In the cell phone market it is well

established. In the utilities market it is not as well known. Different areas and transformers are set up differently. The privacy effort with roaming will be working with many different entities with activity in this space.

- Lee: Why was it put into law when no one knows how it is supposed to work?
- Coop: Don't know why it was put into the law. Likely someone just thought it was a good idea. Reality is that it will probably cost a lot in infrastructure. If everyone must do roaming agreements, it could get very ugly.
- Lee: From a privacy standpoint it is definitely not a good thing.
- IEEE is just one of the other groups working on it. Society of Automotive Engineers is interested in participating. 2030.1 SAE and Electrical Institute are also interested.
- Wed at 3pm est
- NSTIC Team: Amanda Stallings, Ohio PUC (team lead)
 - No report this week.

3. CPNI briefing: Chris Kotting and Erick Soriano

- Erick: Will discuss the enabling legislation which is the Customer Proprietary Network Information (CPNI) statute, then what the FCC has done, and then some of the requirements. Erick is a partner with a law firm at the Georgetown DC office. Is a telecommunications lawyer. Looking to see if the principles from section 222 from the FCC rules can also be applied to the smart grid.
- Section 222 of the Communications Act of 1934 as amended has requirements for how carriers provide services to their customers. It contemplates treatment of different customer information. The most sensitive information, CPNI, is subject to very strict requirements and protections. The customers' data don't really have the same protections as the CPNI information.
- Chris: The subscriber listing information is typically the stuff that gets published in the phone directory. Historically if you had a phone, you had it because you wanted people to be able to find you and call you. You have to opt-out to get an unlisted number.
- Erick: The customer information is not afforded the same privacy protections. Another category that is not given protection is aggregate data, where personal information is stripped off. CPNI is the category that deserves and is given very strict requirements. It is defined as "customer proprietary network information" means-- (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information."
- Length of calls, duration, etc. Is subject to a series of FCC decisions.
- What has the FCC done? Customers must generally protect information.
- Lee: Scope of 222 is for all phone companies?
- Chris: Applied to both traditional and cell phone carriers.
- Erick: FCC recently determined that providers of VoIP over the Internet are also subject to the rules. In 2007? Determined VoIP providers are also covered.
- Lee: Those carriers are also covered under the stored data act and some other acts.
- Erick: Correct. Voice carriers are subject to many statutes including CALEA. Under CPNI rules there is a requirement that for a breach of CPNI, the carrier must report to secret service and the ??? **<Erick, I didn't get this down while taking notes; can you please let us know what goes here?>**. In the telecommunications arena the FBI is involved.

- FCC has established a total service approach so carriers can use and share CPNI data with approval or without approval. Can use w/o customer approval if part of existing customer service. E.g., Verizon offers various services. If they only provided local service to a customer, they can use the CPNI data to market only local options. But if they also provide long distance through another provider, they can also provide marketing about local or long distance without approval.
- Opt-in requires explicit customer consent.
- Opt-out, consent is deemed to be obtained if the customer does not respond, under FCC, within 30 days to a request to use their data.
- If a carrier wants to share data with a 3rd party, opt-in is required.
- If sharing info with joint venture partners, opt-in is required.
- Depending on situation you can use CPNI w/o customer approval, and approval can be done in a variety of ways.
- The FCC has very specific rules requiring giving notice to customers.
- Notification requirements vary for opt-in and opt-out.
- There is no safe harbor for these rules.
- Notification enforcement. In a breach, the carrier within 7 business days, must advise Sec Svc and FBI, but you do not need to notify/advise the customer. Want the law enforcement agencies to do their jobs before the customer is notified. After notifying the FBI/SS, they can contact the customers, but only with the approval of the FBI/SS.
- There are also requirements for records retention. E.g., approvals, notifications, marketing, etc.
- There are filings for the FCC. The CEO/officer must file a certification to the FCC that indicates they have established controls annually.
- If you don't protect CPNI, the FCC can issue a notice of apparent liability and can apply fines to carriers, up to \$150,000 for each violation and continuation for each day of violation. Continuing violations can be very high.
- There is an exemption when a carrier is required to report child pornography without violated CPNI rules.
- The statute and rules are convoluted and not instinctive. But this should give an idea of the approaches that may be considered to be transferred into the smart grid arena.
- Chris: When a carrier can disclose the CPNI, in terms of being disclosed, there is a requirement that a password must be established for the customer. It cannot be based upon any biological factor. In order to obtain your own CPNI, you have to know the password, the backup question, or physically go to the office.
- Erick: Social engineering by data brokers has occurred quite frequently which is why these rules were established.
- Chris: Another aspect is when you have 3rd party service providers, the issue of how and when to release info needed for service; how and when can you release it before the provider can get access to the information. Has pretty much been laid out by the FCC.
- Erick: Talking about making subscriber lists and customer information available to 3rd parties.
- Chris: When a customer wants to change carrier they must provide that verification before the new carrier can get access to the information.
- Erick: IF a customer wants to move to another carrier a customer would want the new carrier to get my information from my old carrier. That data is subject to protection. If AT&T is advised by Verizon that a customer is being moved to Verizon, AT&T cannot do marketing to try and keep them.
- Chris: The wholesale side is forbidden from telling the retaining side about the transition. A protection to give carriers an opportunity to get into the market.
- Glad to answer questions.

- Christine: Concerns process of creating the body of work. Does as situations came up?
- Erick: In 1980s the FCC had rules that related to customer info protection. Act of 1996 amended communications act of 1934. One of provisions (section 222) asked the FCC to implement the act started with a series of decisions. Released 1st order in 1998. All kinds of notes on various grounds; 10th circuit remanded rules. The FCC then subsequently released subsequently additional orders. Latest one was released approx. 2 weeks or months ago.
- Chris: The FCC does not do use case development. They write rules as problems and situations come up.
- Lee: The typical proceeding, in that everyone with skin in the game can send in comments. The FCC then considers and then makes their final decision. Similar to how the FTC makes a decision about something. The FCC got into a lot of trouble with the earlier rules. Later with the pretexting laws, someone petitioned for stronger rules. Was not based upon any type of NIST methodology.
- Chris: Standards and similar are usually not appealable. FCC decisions are, by circuit courts and various others.
- Erick: There is a lot to learn from this situation. Is a process that took root in 1980s, then evolved. Years and years of development of standards that we may be able to apply in the smart grid context. Can see how the filing requirements, notifications, opt-in/opt-out, etc. processes. Can really learn a lot from this.
- Aryeh Fishman/EEU: Thinks it is good to consider. Look at comments that they submitted this summer. Some CPNI rules are very extensive and require a lot of back office functionality. There is a cost to all the rules. Not everything will translate over. There is not consensus that all CPNI rules should be applied.
- Lee: How would utilities feel about the statutory framework (Rule 222) as opposed to the regulatory framework?
- Aryeh Fishman/EEU: Don't think we've posed the question in this way. To extent folks can say CPNI is a good model, his sense is the broader concepts would be better. The whole bureaucratic concepts. This subject has been on the mind of the utilities.
- Chris: Where they DON'T want to go is to carrier to carrier settlement. Don't want to bill each other for roaming charging of PEVs.
- Chris: Has some write-ups and will share them with the mail list.

Thanks,

Rebecca